DANE and SMTP: TLS Protection for SMTP
Using DANE and DNSSEC

Russ Mundy & Wes Hardaker
Parsons
<Russ.Mundy@parsons.com>
<mundy@tislabs.com>
Sending E-Mail Today

1. Sender transmits outgoing email to their mail server, i.e., Mail Transfer Agent (MTA)

2. The sender’s MTA uses the receiver’s DNS “MX” records to find a destination MTA address.

3. The sender’s MTA sends email to the receiver’s MTA address.
Unfortunately, it is possible to create fake MX records, allowing an attacker to pretend to be the right “real” destination.
Solution #1: DNSSEC

DNSSEC ensures that only good DNS records are believable.
Problem #2: Unprotected SMTP

Most SMTP server to server exchanges are unencrypted.

Eavesdropping Is Easy!
Solution #2: TLS-Protected SMTP

SMTP can run over encrypted TLS, but:

- Few server to server exchanges have TLS turned on
- Management of CA Trust Anchors impractical for operators
  - MTA servers don’t normally distribute trust anchor lists
- DANE records are being defined to act as a DNS-based trust anchor
Problem #3: SMTP Man-in-the-Middle

SMTP over TLS uses the “STARTTLS” command
- Attackers “in path” can pretend to be the receiver’s MTA
- Man-in-the-middle allows for “I don’t support STARTTLS”
- Current default policy must be to deliver unencrypted if TLS is unavailable
Solution #3: SMTP over TLS with DANE

A DANE record can indicate you MUST use TLS!
SMTP Over TLS with DNSSEC & DANE

- Protects against MX record forgeries
- Protects against eavesdropping
- Protects against STARTTLS Man-in-the-Middle
- Provides secured X.509 trust-anchors for TLS